(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2003 年12 月18 日 (18.12.2003)

PCT

(10) 国際公開番号
WO 03/105037 A1

(51) 国際特許分類[7]: G06F 17/60

(21) 国際出願番号: PCT/JP02/05582

(22) 国際出願日: 2002 年6 月6 日 (06.06.2002)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について): 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒211-8588 神奈川県 川崎市中原区 上小田中4丁目1番1号 Kanagawa (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 三浦 正之 (MIURA,Masayuki) [JP/JP]; 〒206-0801 東京都 稲城市 大字大丸1405番地 株式会社富士通パソコンシステムズ内 Tokyo (JP).

(74) 代理人: 土井 健二, 外(DOI,Kenji et al.); 〒222-0033 神奈川県 横浜市港北区 新横浜3-9-5 第三東昇ビル 林・土井国際特許事務所 Kanagawa (JP).

(81) 指定国 (国内): JP, US.

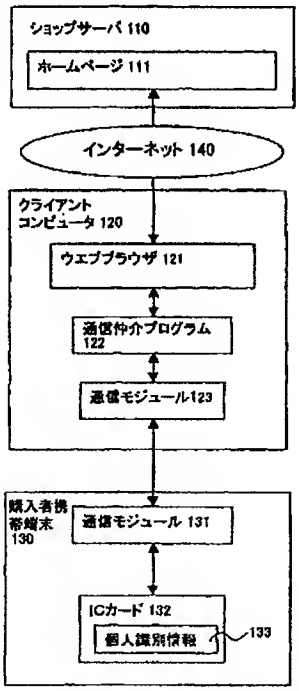
(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: DATA COMMUNICATION MEDIATION APPARATUS COOPERATING WITH PURCHASER MOBILE TERMINAL

(54) 発明の名称: 購入者携帯端末と共働するデータ通信仲介装置



110...SHOP SERVER
111...WEB SITE
140...INTERNET
120...CLIENT COMPUTER
121...WEB BROWSER
122...COMMUNICATION MEDIATION PROGRAM
123...COMMUNICATION MODULE
130...PURCHASER MOBILE TERMINAL
131...COMMUNICATION MODULE
132...IC CARD
133...INDIVIDUAL IDENTIFICATION INFORMATION

(57) Abstract: In the Internet shopping, user-friendly and secure authentication is realized. A client computer (120) is an ordinary personal computer and has a communication medication program (122) activated when paying out in the shopping. A purchaser mobile terminal (130) is, for example, an IC card-equipped mobile telephone which

[続葉有]

WO 03/105037 A1

Is connected to the client computer by radio or the like. The IC card (132) has a crypt processing function and contains electronic certificate and credit card information. When paying out, the communication mediation program, for authentication, receives an electronic certificate from the IC card and transmits it directly to a shop server (110) without leaving it in a local hard disc.

(57) 要約:

インターネット・ショッピングにおいて使い良さとともによりセキュアな認証を実現する。クライアントコンピュータ(120)は、通常のパーソナルコンピュータであり、ショッピングでの支払いのときに起動する通信仲介プログラム(122)をもつ。購入者携帯端末(130)は、たとえばICカードつき携帯電話であり、クライアントコンピュータと無線などにより接続される。ICカード(132)は、暗号処理能力をもち、あらかじめ電子証明書やクレジットカード情報をストアしている。支払いのとき、通信仲介プログラムは認証のためにICカードから電子証明書を受け取ってそれをローカルのハードディスクに残したりせずに直接ショップサーバ(110)に送る。

明細書

購入者携帯端末と共働するデータ通信仲介装置

[技術分野]

本発明は、認証処理に関し、特にインターネットショッピングにおける個人認証および決済認証処理のデータ通信を仲介するデータ通信仲介プログラムおよび前記データ通信を仲介する通信仲介装置を有するクライアントコンピュータに関する。

[背景技術]

インターネット上に作成されている、個人、法人等のホームページから商品やサービス等のアイテムを購入し、代金支払いの決済手続きを行う一連の行為はインターネットショッピングとして現在広く行われている。本明細書では、サービスを購入者が選択可能な商品の１つとみなし、商品やサービス等のアイテムを簡単のために商品として説明する。

購入者はまずインターネットに接続されたパーソナルコンピュータ（以下 PC と略す）などのクライアントコンピュータから、ウェブブラウザを利用しショップのホームページに掲載された商品を閲覧し、購入する商品を選択する。購入する商品が決定したら、その旨を告げ購入手続きに入る。この購入手続きにおいて、購入者の身元を明らかにし、本当に取引を行う意思があるかを確認するための個人認証と、購入者によって支払いが行われたか、もしくは購入者に支払能力があるかを確認する決済認証が行われる。個人認証は、購入者個人を特定するための情報である個人情報を基に行われ、決済認証は、クレジットカード番号や銀行口座番号などの決済情報を基にして行われる。本明細書では、以後個人情報と決済情報を併せて個人識別情報と呼ぶ。ショップは、上記個人認証、決済認証の結果が良好なら、商品を出荷し、こうして購入手続きは終了する。

このようにインターネットショッピングにおいては、個人識別情報が重要な役割を担っている。

しかしながら、購入者は通常、インターネットショッピングをＰＣなどのクライアントコンピュータで行う場合、個人認証や決済認証が必要な場面において、クライアントコンピュータ上で個人識別情報を入力している。一般にＰＣなどのクライアントコンピュータでは入力された個人識別情報がハードディスクに格納されるため、悪意を持った第三者がハードディスクの情報を直接読み出したり、ネットワークを介して端末装置に侵入して情報を読み出したり、本人が端末装置を離れている間に残っている履歴を盗み見したりして、アカウント、パスワード、クレジットカード番号、住所、電話番号、といった個人識別情報が購入者以外の第三者に簡単に漏洩してしまう。その結果、第三者が本人になりすまして商品の購入をする、「なりすまし」が起きる危険性がある。

一方、購入者が携帯電話を含めた通信機能を備えた購入者携帯端末でインターネットショッピングを行うこともある。この場合、個人識別情報などのデータはハードディスクのような取り出し可能な独立した装置に格納されるのではなく、購入者携帯端末内部のメモリに格納されるため、ＰＣなどのクライアントコンピュータと比較すると個人識別情報の漏洩による「なりすまし」が起きる可能性は低い。だが、購入者携帯端末の画面は一般に小さいため、購入者は商品の選択や比較をするために、画面の切り替えやスクロールなどをしなければならず、手間がかかり、またPC等と比較すると通信速度が遅い場合が多く、画像などのデータをダウンロードするのに時間がかかり、通信料金が高い、等の理由から、購買を決定するのに十分な情報が得にくい課題がある。

したがって、購入者による商品の閲覧には、一画面に複数の画像が表示でき、その詳細な説明が得られるだけの大きさを備えた画面と高速な通信機能を備え、購買の決定に十分な情報が得られるクライアントコンピュータを使用し、但し、クライアントコンピュータのハードディスクのような第三者にデータが漏洩する可能性のある場所に個人識別情報が格納されず、結果「なりすまし」を防止できる個人認証、決済認証処理が必要である。

[発明の開示]

本発明の目的は、インターネットショッピングにおいて、画面が大きく、操作性のよいＰＣなどのクライアントコンピュータを使用して、商品の選択を行いながら、個人認証、決済認証の際要求される個人識別情報をクライアントコンピュータから獲得するのではなく、より情報が第三者に漏洩しにくい購入者携帯端末から獲得し、「なりすまし」を防止する個人認証、決済認証処理を行うことができる環境を提供することにある。

上記目的を達成するために、サーバにコンピュータネットワークを介して接続可能なクライアントコンピュータに、個人識別情報が格納された購入者携帯端末と共働して、個人識別処理を実行させる通信仲介プログラムにおいて、前記個人識別処理は、前記サーバからの個人識別情報要求信号に応答して、当該個人識別情報要求信号を前記購入者携帯端末に転送する手順と、前記購入者携帯端末に格納される前記個人識別情報であって、前記購入者携帯端末が前記個人識別情報要求信号に応答して前記クライアントコンピュータに送信する前記個人識別情報を、前記サーバに転送する手順とを有することを特徴とするプログラムを提供する。

上記発明によれば、大きな画面でより鮮明かつ詳細な情報が得られ、操作性も良好なPCなどのクライアントコンピュータを利用して商品の閲覧、選択が行われ、第三者に個人識別情報が漏洩する可能性がＰＣなどの端末装置より低い、購入者携帯端末に格納された個人識別情報で個人認証、決済認証が行われることで、「なりすまし」を防止することができる。

[図面の簡単な説明]

図１は、本発明の実施例における構成例を示す図である。

図２は、電子署名入りデータの信頼性確認の例を示す図である。

図３は、第一の実施例でのフローチャートである。

図４、５は、第二の実施例でのフローチャートである。

図６、７、８、９は、第三の実施例でのフローチャートである。

[発明を実施するための最良の形態]

以下、本発明の実施例について図面に従って説明する。しかしながら、本発明の技術的範囲はかかる実施例によって限定されるものではなく、特許請求の範囲に記載された発明とその均等物に及ぶものである。

図１は、本発明の実施例における構成例を示す図である。

ショップサーバ１１０は、ショップのホームページ１１１を提供するサーバである。クライアントコンピュータ１２０には、前記ホームページを閲覧するためのウェブブラウザ１２１と本発明の通信仲介プログラム１２２とがインストールされ、更に通信モジュール１２３が備えられている。ウェブブラウザ１２１と通信仲介プログラム１２２は同じオペレーティングシステム上で実装されており、ウェブブラウザ１２１から通信仲介プログラム１２２を起動できる。

ショップサーバ１１０とクライアントコンピュータ１２０は、インターネット１４０を介して接続される。

購入者携帯端末１３０には、前記クライアントコンピュータ１２０内の通信モジュール１２３とデータ通信が可能な通信モジュール１３１、個人識別情報１３３を含んだＩＣカード１３２が備えられている。通信モジュール１２３、通信モジュール１３１の一例としては、ＢｌｕｅＴｏｏｔｈや、ＩＥＥＥ８０２．１１ｂ用無線モジュールなどが好ましい。

ＩＣカード１３２は、ＩＣチップが内蔵されたチップカードであり、演算機能、磁気カードよりも大容量のメモリ、そして高いセキュリティ機能を持つ。セキュリティ機能には、演算機能を使ってカード外部とのデータのやり取りを暗号化、復号化しデータの盗聴を防止する暗号機能や、耐タンパー性（外部からの物理的攻撃に抵抗し、解析されにくい特性）により、ＩＣカードを分解し解析しようとすると、チップそのものが回路的に破壊されるような、偽造、変造、改ざん等を防止する機能がある。このようにして、ＩＣカード１３２内の個人識別情報１３３そのものだけでなく、ＩＣカード１３２と外部装置との個人識別情報１３３のデータのやり取りも保護されており、第三者に個人識別情報１３３が漏洩する可能性はＰＣよりも低い。

個人識別情報１３３には、個人情報として、ＣＡ電子署名入り購入者携帯端末電子証明書と購入者携帯端末個人鍵が、決済情報として、クレジットカード決済

をするのに必要なクレジットカード情報が格納されている。なお例えば他に、個人情報として、住所、氏名、年齢、電話番号、血液型や、決済情報として、銀行口座番号等が格納されていてもよい。

ＣＡ電子署名入り購入者携帯端末電子証明書は、購入者携帯端末１３０がＣＡ（Ｃｅｒｔｉｆｉｃａｔｉｏｎ Ａｕｔｈｏｒｉｔｙ、または認証局）から発行を受けた電子証明書にＣＡ電子署名が付加されたものである。購入者携帯端末電子証明書には、購入者携帯端末公開鍵が含まれ、前記購入者携帯端末公開鍵が確かに購入者携帯端末本人のものであることはＣＡにより保証されている。

電子署名とは、公開鍵暗号化方式を利用しており、基になるデータを一定のアルゴリズム（ハッシュ関数）に従って変換したメッセージダイジェストを、署名者の個人鍵で暗号化したもので、この基になるデータと対にして利用される。ネットワークを介して受信した電子署名入りデータの信頼性は図２のようにして確認できる。

図２は、電子署名入りデータの信頼性確認の例を示す図である。本例は、ＣＡ電子署名入り購入者携帯端末電子証明書を受信した場合である。受信側２２０では、ＣＡ電子署名２２２をＣＡ公開鍵２３０で復号化することにより得られるメッセージダイジェスト２２５と、購入者携帯端末電子証明書２２１をハッシュ関数２２３で変換して得られるメッセージダイジェスト２２４を比較する。結果が同じであれば、伝送途中でデータが改ざんされておらず、またＣＡ電子署名２２２が確かに購入者携帯端末電子証明書２２１に対してなされたものであることがわかる。ＣＡの存在が信頼できることから、受信した購入者携帯端末電子証明書２２１の信頼性が確立する。なお、基になるデータは電子証明書に限られず、また署名者もＣＡに限られないが、その際は、図２の購入者携帯端末電子証明書、ＣＡ電子署名、ＣＡ公開鍵をそれぞれ対応するデータ、対応する署名者の電子署名、対応する署名者の公開鍵として読みかえればよい。電子署名入り文書の信頼性確認は、本明細書においてしばしば行われるため、以後この確認手続きを「電子署名確認」と呼ぶ。

図３は、第一の実施例でのフローチャートである。第一の実施例は、購入者携帯端末電子証明書を用いて個人認証を行い、クレジットカード情報を用いて決済

認証を行うインターネットショッピングにおいて、通信仲介プログラムがショップサーバからの個人情報要求を購入者携帯端末へ転送し、購入者携帯端末から応答されたＣＡ電子署名入り購入者携帯端末電子証明書をショップサーバへ転送し、ショップサーバからの決済情報要求を購入者携帯端末へ転送し、購入者携帯端末から応答されたクレジットカード情報をショップサーバへ転送し、それぞれの認証処理が行われる例である。

本実施例の前提として、ショップサーバはＣＡ公開鍵３０１を取得済みであるとする。また、購入者携帯端末１３０内ＩＣカードには、個人識別情報として、ＣＡ電子署名入り購入者携帯端末電子証明書３０２、クレジットカード情報３０３が格納されている。

まず購入者は、大画面で情報が得やすく操作性にも優れたクライアントコンピュータ１２０のウェブブラウザ１２１を使用して、インターネット１４０を介してショップサーバ１１０にアクセスし、ショップサーバ１１０に格納された販売者のホームページ１１１を閲覧し、商品の選択を行う（Ｓ１）。購入したい商品が決定したら、購入者は注文情報と購入意思をショップサーバへ送信する（Ｓ２）。ステップＳ２は例えば、事前に商品が選択されており、購入手続きに進むためにホームページに用意されたボタンをクリックすることで、それまでに選択された商品を購入する意思があると判定されることで実現されている。前記注文情報には、購入する商品と個数の情報が含まれる。

ショップサーバ１１０では、クライアントコンピュータ１２０へ購入手続き開始を通知する（Ｓ３）。ステップＳ３では、例えば購入開始を示す特別なＨＴＭＬタグが埋められたページが送信されるとする。前記購入手続き開始通知を受け、通信仲介プログラムが起動され、転送を開始する（Ｓ４）。ステップＳ４は、例えばウェブブラウザ１２１が前記購入開始を示す特別なＨＴＭＬタグを発見した際に通信仲介プログラム１２２を起動すればよい。次にショップサーバ１１０は、個人認証をするために、個人情報要求をクライアントコンピュータ１２０に送信する（Ｓ５）。通信仲介プログラム１２２は、前記個人情報要求を、通信モジュール１２３を介して購入者携帯端末１３０へ転送する（Ｓ６）。前記個人情報要求に対し、購入者携帯端末１３０では、ＩＣカード１３２が格納された個人識別

情報１３３からＣＡ電子署名入り購入者携帯端末電子証明書３０２を応答し、前記ＣＡ電子署名入り購入者携帯端末電子証明書は通信モジュール１３１を介して、クライアントコンピュータ１２０へ送信される（Ｓ７）。通信仲介プログラム１２２は、クライアントコンピュータのハードディスクにＣＡ電子署名入り購入者携帯端末電子証明書３０２を書き込むことなく、ショップサーバ１１０へ前記ＣＡ電子署名入り購入者携帯端末電子証明書を転送する（Ｓ８）。ショップサーバ１１０では、ＣＡ公開鍵３０１を使用して、ＣＡ電子署名入り購入者携帯端末電子証明書３０２の電子署名確認を行う（Ｓ９）。電子署名確認の手順は、図２に述べられている。ステップＳ９にて、購入者携帯端末電子証明書の信頼性が確立すると、個人認証は完了する。

ステップＳ９にて個人認証が成功すると、続いてショップサーバ１１０は、クライアントコンピュータ１２０に対して、決済情報を要求する（Ｓ１０）。通信仲介プログラム１２２は、前記決済情報要求を購入者携帯端末１３０へ転送する（Ｓ１１）。前記決済情報要求に対し、購入者携帯端末１３０内ＩＣカード１３２はクレジットカード情報３０３を応答し、前記クレジットカード情報は通信モジュール１３１を介して、クライアントコンピュータ１２０へ送信される（Ｓ１２）。通信仲介プログラム１２２は、クライアントコンピュータのハードディスクにクレジットカード情報３０３を書き込むことなく、前記クレジットカード情報をショップサーバへ転送する（Ｓ１３）。ショップサーバでは、クレジットカード情報３０３を基に与信審査を行い、決済認証を完了する（Ｓ１４）。続いて、図示はしないが、決済認証結果による商品の出荷処理を経て、第一の実施例は終了する。

なおステップＳ１２でのクレジットカード情報３０３の応答は、ショップサーバ以外の第三者に盗聴されないよう暗号化を施すことが望ましい。例えば、購入者携帯端末１３０が、ショップサーバ公開鍵を取得していれば、当該ショップサーバ公開鍵を用いて暗号化すればよい。また本実施例では、個人認証と決済認証を分けて実施している例であるが、個人情報要求と決済情報要求が一度に行われることもある。その場合、ステップＳ７において、購入者携帯端末１３０内のＩＣカード１３２がＣＡ電子署名入り購入者携帯端末電子証明書３０２とクレジッ

トカード情報３０３を同時に応答すればよい。

本実施例により、商品の選択には画面の大きなクライアントコンピュータを使用しながら、購入者携帯端末内ＩＣカードに格納された、第三者に漏洩しにくい個人識別情報を使用して、個人認証や決済認証を完了することができる。したがって、クライアントコンピュータのハードディスクに個人識別情報を残すことなく、インターネットショッピングを行うことができ、インターネットショッピングをしやすい環境とハードディスクからの個人識別情報の読み出しによる成りすまし防止を両立することができる。

図４、５は、第二の実施例でのフローチャートである。図４における携帯端末１３０、クライアントコンピュータ１２０、ショップサーバ１１０のフロー下端、４０７、４０８、４０９はそれぞれ図５の対応するフローの上端と一続きであり、したがって二図を合わせて説明する。第二の実施例は、購入者携帯電子証明書を用いて個人認証を行い、クレジットカード情報を用いて決済認証を行うインターネットショッピングにおいて、通信仲介プログラムがショップサーバからの個人情報要求を購入者携帯端末へ転送し、購入者携帯端末から応答されたＣＡ署名入り購入者電子署名をショップサーバへ転送し、ショップサーバからの決済情報要求を購入者携帯端末へ転送し、購入者携帯端末から応答された共通鍵暗号化方式を用いて暗号化された決済情報をショップサーバへ転送し、それぞれ認証処理が行われる例である。

本実施例の前提として、購入者携帯端末１３０内ＩＣカードには、個人識別情報として、ＣＡ電子署名入り購入者携帯端末電子証明書３０２、クレジットカード情報３０３が、ショップサーバ１１０はＣＡ電子署名入りショップサーバ電子証明書４０１を得ている。また購入者携帯端末、ショップサーバはともにＣＡ公開鍵３０１を取得済みである。

図４において、まず購入者は、大画面で情報が得やすく操作性にも優れたクライアントコンピュータ１２０のウェブブラウザ１２１を使用して、インターネット１４０を介してショップサーバ１１０にアクセスし、ショップサーバ１１０に格納された販売者のホームページ１１１を閲覧し、商品の選択を行う（Ｓ１）。購入したい商品が決定したら、購入者は注文情報４０２と購入の意思をショップ

サーバへ送信する（Ｓ２）。ステップＳ２は例えば、購入手続きに進むためにホームページに用意されたボタンをクリックすることで、それまでに選択された商品を購入する意思があると判定されることで実現されている。注文情報４０２は、購入する商品と個数の情報である。

ショップサーバ１１０では、クライアントコンピュータ１２０へ購入手続き開始を通知する（Ｓ３）。ステップＳ３では、例えば購入開始を示す特別なＨＴＭＬタグが埋められたページが送信されるとする。前記購入手続き開始通知を受け、通信仲介プログラムが起動され、転送を開始する（Ｓ４）。ステップＳ４は、例えばウェブブラウザ１２１が前記購入開始を示す特別なＨＴＭＬタグを発見した際に通信仲介プログラム１２２を起動すればよい。

ショップサーバ１１０はクライアントコンピュータ１２０へ個人情報要求とＣＡ電子署名入りショップサーバ電子証明書４０１を送信する（Ｓ１５）。通信仲介プログラム１２２は購入者携帯端末１３０へ前記個人情報要求及びＣＡ電子署名入りショップサーバ電子証明書４０１を転送する（Ｓ１６）。購入者携帯端末１３０内ＩＣカード１３２は、ＣＡ公開鍵３０１を使用して、ＣＡ電子署名入りショップサーバ電子証明書４０１の電子署名確認を行う（Ｓ１７）。ステップＳ１７にて、ショップサーバ電子証明書の信頼性が確立すると、ショップサーバ認証は完了する。

ステップＳ１７でショップサーバ認証が済むと、前記個人情報要求に対し購入者携帯端末１３０内のＩＣカード１３２はＣＡ電子署名入り購入者携帯端末電子証明書３０２を応答し、前記ＣＡ電子署名入り購入者携帯端末電子証明書はクライアントコンピュータ１２０へ送信される（Ｓ１８）。通信仲介プログラム１２２は、クライアントコンピュータ１２０のハードディスクにＣＡ電子署名入り購入者携帯端末電子証明書３０２を書き込むことなく、ショップサーバ１１０へ前記ＣＡ電子署名入り購入者携帯端末電子証明書を転送する（Ｓ１９）。ショップサーバ１１０は、ＣＡ電子署名入り購入者携帯端末電子証明書３０２の電子署名確認を行う（Ｓ２０）。ステップＳ２０にて、購入者携帯端末電子証明書の信頼性が確立すると、個人認証が完了する。ステップＳ２０で購入者携帯端末電子証明書の信頼性が確立したので、後の使用のため前記購入者携帯端末電子証明書に

含まれる購入者携帯端末公開鍵４０３を保存する。

次にショップサーバ１１０は、共通鍵暗号化方式で以降の通信を暗号化するために共通鍵に相当する、セッション鍵４０４を作成する（Ｓ２１）。ショップサーバ１１０は、購入者携帯端末公開鍵４０３でセッション鍵４０４および注文情報４０２を暗号化し、クライアントコンピュータへ暗号化されたセッション鍵４０５と暗号化された注文情報４０６を送信する（Ｓ２２）。購入者携帯端末公開鍵４０３で暗号化することで、セッション鍵４０４および注文情報４０２は購入者携帯端末個人鍵を持っていないと取り出せず、事実上それは購入者携帯端末でしか復号化できない。通信仲介プログラム１２２は、購入者携帯端末１３０へ暗号化されたセッション鍵４０５と暗号化された注文情報４０６を転送する（Ｓ２３）。購入者携帯端末１３０内ＩＣカードは、購入者携帯端末の個人鍵を使用して暗号化されたセッション鍵４０５と暗号化された注文情報４０６を復号化し、セッション鍵４０４、注文情報４０２を取り出す（Ｓ２４）。

これより図５である。続いて、購入者携帯端末１３０内ＩＣカード１３２は、購入者に購入商品をクライアントコンピュータ上で確認させるために、非転送フラグ付きで、注文情報４０２を応答し、前記注文情報は、通信モジュール１３１を介しクライアントコンピュータ１２０へ送信される（Ｓ２５）。この非転送フラグは、仲介プログラムに転送させたくないデータがある場合に使用される。非転送フラグは例えば、非転送フラグを示す特殊なＨＴＭＬタグが埋められたページが送信されることで実現される。通信仲介プログラム１２２は非転送フラグを発見し、注文情報４０２をウェブブラウザ１２１に表示させ、購入者に前記注文情報を最終確認させ、最終確認結果をブラウザ１２１から受け取ると、購入がキャンセルされたのでなければ、決済情報要求を購入者携帯端末１３０に送信する（Ｓ２６）。

購入者携帯端末１３０内のＩＣカード１３２は、前記決済情報要求に対し、クレジットカード情報３０３をセッション鍵４０４で暗号化した暗号化されたクレジットカード情報５０１を応答し、前記暗号化されたクレジットカード情報は、クライアントコンピュータへ送信される（Ｓ２７）。通信仲介プログラム１２２は、クライアントコンピュータ１２０のハードディスクに暗号化されたクレジッ

トカード情報５０１を書き込むことなく、ショップサーバ１１０へ前記暗号化されたクレジットカード情報を転送する（Ｓ２８）。ショップサーバ１１０では、暗号化されたクレジットカード情報５０１が復号化され、クレジットカード情報３０３が取り出される（Ｓ２９）。そして、クレジットカードの与信審査をもって決済認証が完了する（Ｓ３０）。その後、図示はしないが、決済認証結果による商品の出荷処理を経て、第二の実施例は終了する。

本実施例により、商品の選択には画面の大きなクライアントコンピュータを使用しながら、購入者携帯端末内ＩＣカードに格納された、第三者に漏洩しにくい個人識別情報を使用し、クライアントコンピュータに個人識別情報を残すことなく、さらにショップサーバと購入者携帯端末間の通信をセッション鍵で暗号化し、個人認証や決済認証を完了することができる。したがって、インターネットショッピングをしやすい環境を保ちつつ、クライアントコンピュータのハードディスクからの個人識別情報の読み出しによる成りすましを防止するだけでなく、購入者携帯端末、クライアントコンピュータ、ショップサーバ間の通信盗聴による個人識別情報漏洩による成りすましも防止することができる。

図６、７、８、９は、第三の実施例でのフローチャートである。第二の実施例における図４と図５の関係と同じく、図６のフロー下端と図７のフロー上端、図７のフロー下端と図８のフロー上端、図８のフロー下端と図９のフロー上端は一続きになっており、したがって四図を合わせて説明する。第三の実施例では、ＳＥＴ（Ｓｅｃｕｒｅ　Ｅｌｅｃｔｒｏｎｉｃ　Ｔｒａｎｓａｃｔｉｏｎ）という既存のクレジットカード決済の標準規格として開発された仕組みに本発明を適用した例である。第三の実施例は、購入者携帯端末電子証明書を用いて個人認証を行い、クレジットカード情報を用いて決済認証を行うインターネットショッピングにおいて、通信仲介プログラムがショップサーバからの個人情報要求を購入者携帯端末に転送し、購入者携帯端末から応答されたＣＡの電子署名入り購入者電子証明書をショップサーバへ転送し、ショップサーバからの決済情報要求を購入者携帯端末へ転送し、購入者携帯端末から応答されたカード会社サーバ公開鍵で暗号化されたクレジットカード情報含むデータをショップサーバに転送し、それぞれ認証処理が行われる例である。

本実施例の前提として、購入者携帯端末１３０は、ウオレットと呼ばれる、通常ＳＥＴにおいては購入者のＰＣで実行されるソフトウエアの機能を処理することができるとする。また購入者携帯端末１３０はＣＡ電子署名入り購入者携帯端末電子証明書３０２を、ショップサーバ１１０はＣＡ電子署名入りショップサーバ電子証明書４０１を、カード会社サーバ１５０はＣＡ電子署名入りカード会社サーバ電子証明書６０１を得ている。また購入者携帯端末１３０、ショップサーバ１１０、カード会社サーバ１５０はともにＣＡ公開鍵３０１を取得済みである。

あらかじめカード会社サーバは、ショップサーバへＣＡ電子署名入りカード会社サーバ電子証明書４１０を送信する（Ｓ３１）。

図６において、まず購入者は、大画面で情報が得やすく操作性にも優れたクライアントコンピュータ１２０のウェブブラウザ１２１を使用して、インターネット１４０を介してショップサーバ１１０にアクセスし、ショップサーバ１１０に格納された販売者のホームページ１１１を閲覧し、商品の選択を行う（Ｓ１）。購入したい商品が決定したら、購入者は注文情報４０２と購入の意思をショップサーバへ送信する（Ｓ２）。ステップＳ２は例えば、購入手続きに進むためにホームページに用意されたボタンをクリックすることで、それまでに選択された商品を購入する意思があると判定されることで実現されている。注文情報４０２は、購入する商品と個数の情報である。

ショップサーバ１１０では、クライアントコンピュータ１２０へ購入手続き開始を通知する（Ｓ３）。ステップＳ３では、例えば購入開始を示す特別なＨＴＭＬタグが埋められたページが送信されるとする。前記購入手続き開始通知を受け、通信仲介プログラムが起動され、転送を開始する（Ｓ４）。

ショップサーバ１１０は、クライアントコンピュータ１２０へＣＡ電子署名入りカード会社サーバ電子証明書６０１、ＣＡ電子署名入りショップサーバ電子証明書４０１、注文情報４０２を送信する（Ｓ３２）。通信仲介プログラム１２２は、購入者携帯端末１３０へＣＡ電子署名入りカード会社サーバ電子証明書６０１、ＣＡ電子署名入りショップサーバ電子証明書４０１、注文情報４０２を転送する（Ｓ３３）。

購入者携帯端末１３０内ＩＣカード１３２は、ＣＡ公開鍵３０１を使用して、

ＣＡ電子署名入りショップサーバ電子証明書４０１の電子署名確認を行い、ショップサーバ認証を行う（Ｓ３４）。認証が成功したら、ショップサーバ電子証明書に含まれるショップサーバ公開鍵６０２を保存する。続いてＣＡ公開鍵３０１を使用して、ＣＡ電子署名入りカード会社サーバ電子証明書６０１の電子署名確認も行い、カード会社サーバ認証を行う（Ｓ３５）。認証が成功したら、カード会社サーバ電子証明書に含まれるカード会社サーバ公開鍵６０３を保存する。次に購入者携帯端末１３０内ＩＣカード１３２は注文情報４０３を基データとして購入者携帯端末電子署名を作成し、購入者携帯端末電子署名入り注文情報６０４を作成する（Ｓ３６）。前記購入者携帯端末電子署名はこの注文が確かに購入者によってなされたことを確定するためのもので、これにより購入者は言い逃れができない。

これより図７である。さらに購入者携帯端末１３０内のＩＣカード１３２は、クレジットカード情報３０３と注文情報４０２から作成したメッセージダイジェストをまとめたデータを決済情報とし、カード会社サーバ公開鍵６０３で暗号化し、暗号化された決済情報７０１を作成する（Ｓ３７）。これにより、クレジットカード情報３０３はクレジットカード会社の個人鍵でのみ復号化でき、ショップにおいて盗み見られることはない。こうしてＣＡ電子署名入り購入者携帯端末電子証明書３０２、購入者携帯端末電子署名入り注文情報６０４、暗号化された決済情報７０１が、クライアントコンピュータ１２０へ送信される（Ｓ３８）。通信仲介プログラム１２２は、ショップサーバ１１０へＣＡ電子署名入り購入者携帯端末電子証明書３０２、購入者携帯端末電子署名入り注文情報６０４、クレジットカード会社サーバ公開鍵にて暗号化された決済情報７０１を転送する（Ｓ３９）。

ショップサーバ１１０では、ＣＡ電子署名入り購入者携帯端末電子証明書３０２の電子署名確認を行い、個人認証を行う（Ｓ４０）。認証に成功したら、購入者携帯端末公開鍵４０３を保存する。次に購入者携帯端末電子署名入り注文情報６０４の電子署名確認を行う（Ｓ４１）。比較の結果が同じであれば、注文情報が信頼でき、ショップは購入者に提供すべき商品名や個数などがわかる。ここで、注文に対して購入者とショップの同意が取れたことの証しとして、ショップサー

バは、注文情報４０３から作成したメッセージダイジェストを基データとしてショップサーバ電子署名を作成し、ショップサーバ電子署名入りメッセージダイジェスト７０２を作成する（Ｓ４２）。そして、ショップサーバ１１０はカード会社サーバ１５０へ、ＣＡ電子署名入り購入者携帯端末電子証明書３０２、ＣＡ電子署名入りショップサーバ電子証明書４０１、ショップサーバ電子署名入りメッセージダイジェスト７０２、カード会社サーバ公開鍵６０３で暗号化された決済情報７０１を送信する（Ｓ４３）。注文情報を直接送るのではなく、メッセージダイジェストを送ることによって、カード会社サーバには注文の内容は伝わらず、単に合計金額と、購入者とショップが注文に対して同意が取れているという事実だけが伝わることになる。

カード会社サーバ１５０では、ＣＡ電子署名入りショップサーバ電子証明書４０１の電子署名確認を行い、ショップサーバ認証を行う（Ｓ４４）。認証が成功したら、ショップサーバ電子証明書に含まれるショップサーバ公開鍵６０２を保存する。

これより図８である。続いてカード会社サーバ１５０は、ＣＡ電子署名入り購入者携帯端末電子証明書３０２の電子署名確認を行い、個人認証を行う（Ｓ４５）。認証が成功したら、購入者携帯端末電子証明書に含まれる購入者携帯端末公開鍵４０３を保存する。次にカード会社サーバ個人鍵で暗号化された決済情報７０１を復号する（Ｓ４６）。決済情報からクレジットカード情報を取り出し、与信審査を行って決済認証を行う（Ｓ４７）。さらに、ショップサーバ電子署名入りメッセージダイジェスト７０２の電子署名確認を行い、購入者とショップが注文に同意しているかを確認する（Ｓ４８）。カード会社サーバ１５０は直接の注文情報４０３は把握できないが、販売者がステップＳ２５にて購入者からの注文情報４０３の内容を確認したことを確認することができる。次に、送信されたメッセージダイジェスト５０６と決済情報３０４を復号化した際に得られる注文情報４０３から作成したメッセージダイジェストを比較する（Ｓ４９）。これは、決済される金額が注文情報４０３に基づくものであるかを確認するためである。比較の結果が同じであれば、ショップが請求した金額が確かに購入者の注文情報４０３に基づくものであると確認できる。ショップに審査結果を通知するために、カ

ード会社サーバ電子署名入り審査結果８０１を作成する（Ｓ５０）。カード会社サーバ１５０は、ショップサーバ１１０へ、カード会社サーバ電子署名入り審査結果８０１、カード会社サーバ公開鍵６０３で暗号化された決済情報７０１を送信する（Ｓ５１）。

これより図９である。ショップサーバ１１０では、カード会社サーバ電子署名入り審査結果８０１の電子署名確認を行い、審査結果をもって、決済認証を完了する（Ｓ５２）。購入者に伝えるため、審査結果を基データとしてショップサーバ電子署名を作成し、ショップサーバ電子署名入り審査結果９０１を作成する（Ｓ５３）。クライアントコンピュータ１２０へ、ショップサーバ電子署名入り審査結果９０１、カード会社サーバ公開鍵６０３で暗号化された決済情報７０１を送信する（Ｓ５４）。

通信仲介プログラム１２２は、購入者携帯端末１３０へ、ショップサーバ電子署名入り審査結果９０１、暗号化された決済情報７０１を転送する（Ｓ５５）。

購入者携帯端末１３０内ＩＣカード１３２は、ショップサーバ電子署名４０４入り審査結果の電子署名確認を行い、信頼性を確認した後、審査結果を確認する（Ｓ５６）。このとき、購入者携帯端末からクライアントコンピュータへすべての処理の終了が通知され、例えばその通知がブラウザに表示されてもよい。これにより第三の実施例は終了する。

本実施例により、商品の選択には画面の大きなクライアントコンピュータを使用しながら、購入者携帯端末内ＩＣカードに格納された、第三者に漏洩しにくい個人識別情報を使用し、さらにＳＥＴの仕組みを既存のまま利用して、個人認証や決済認証を完了することができる。したがって、インターネットショッピングをしやすい環境を保ちつつ、クライアントコンピュータのハードディスクからの個人識別情報の読み出しによる「成りすまし」を防止するだけでなく、購入者携帯端末、クライアントコンピュータ、ショップサーバ、カード会社サーバ間の通信盗聴による個人識別情報漏洩による「成りすまし」も防止することができ、さらにＳＥＴの設備が整備されていれば、そのまま用いることができ、過去の設備投資を無駄にしなくて済むメリットがある。

以上述べてきた本発明の実施例は、ショップサーバで行われる購入処理に伴う

認証処理に限定されるものではなく、他の処理に伴う認証処理にも適用が可能である。

［産業上の利用の可能性］

以上説明したように本発明によれば、インターネットショッピングにおいて、商品の選択には画面の大きなクライアントコンピュータを使用しながら、第三者によってデータが読み出される可能性のあるクライアントコンピュータのハードディスクに、購入者の個人識別情報を格納することなく、個人認証、決済認証が完了する環境を提供することができ、なりすましを防止することができる。さらに、購入者携帯端末内のＩＣカードの持つ暗号化機能を利用すれば、サーバと購入者携帯端末間の通信データも保護でき、個人識別情報が盗聴されることによる成りすましも防止可能である。

請求の範囲

1. サーバにコンピュータネットワークを介して接続可能なクライアントコンピュータに、個人識別情報が格納された携帯端末と共働して、個人識別処理を実行させるプログラムにおいて、

前記個人識別処理は、

前記サーバからの個人識別情報要求信号に応答して、当該個人識別情報要求信号を前記携帯端末に転送する手順と、

前記携帯端末に格納される前記個人識別情報であって、前記携帯端末が前記個人識別情報要求信号に応答して前記クライアントコンピュータに送信する前記個人識別情報を、前記サーバに転送する手順とを有することを特徴とするプログラム。

2. 請求項１において、

前記個人識別処理は、

受信したデータに非転送フラグが含まれている時は、当該受信データを転送しない手順を有することを特徴とするプログラム。

3. 請求項１において、

前記個人識別処理に先立ち、

前記サーバに接続して前記クライアントコンピュータにインストールされているブラウザによる電子商取引のセッション中に、前記ショップサーバからの指令に対応する起動命令に応答して、起動する手順を前記クライアントコンピュータに実行させることを特徴とするプログラム。

4. 請求項１において、

前記個人識別情報は、前記電子商取引を行う個人を特定する個人情報と、当該電子商取引を行う個人の決済情報のいずれか一方を少なくとも有することを特徴とするプログラム。

5. 請求項３において、

前記個人情報は、前記携帯端末の個人電子証明書と当該個人電子証明書の認証局の電子署名とを有することを特徴とするプログラム。

6. 請求項３において、

前記決済情報は、クレジットカードＩＤまたは金融機関の引落口座ＩＤのいずれか一つを有することを特徴とするプログラム。

7. 請求項１において、

前記携帯端末が前記個人識別情報要求信号に応答して前記クライアントコンピュータに送信する前記個人識別情報は、所定の暗号鍵に従って暗号化されていることを特徴とするプログラム。

8. 請求項６において、

前記所定の暗号鍵は、前記サーバ若しくはクレジットカード会社の公開鍵、または前記電子商取引のセッション時に作成されたセッション鍵のいずれかであることを特徴とするプログラム。

9. サーバにコンピュータネットワークを介して接続可能なクライアントコンピュータであって、

前記サーバからの個人識別情報要求信号に応答して、当該個人識別情報要求信号を個人識別情報が格納された携帯端末に転送する手段と、

前記携帯端末に格納される前記個人識別情報であって、前記携帯端末が前記個人識別情報要求信号に応答して当該クライアントコンピュータに送信する前記個人識別情報を、前記サーバに転送する手段と、

を有することを特徴とする、前記携帯端末と共働する個人識別処理を行うクライアントコンピュータ。

図1

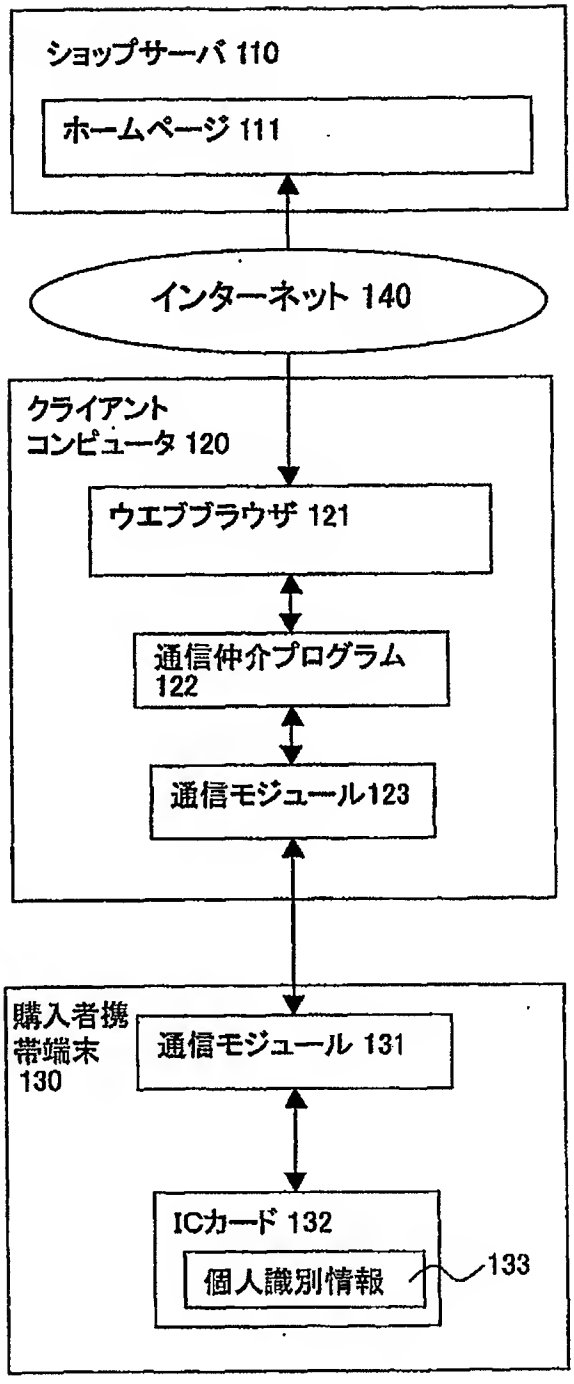

ショップサーバ 110
ホームページ 111
インターネット 140
クライアント
コンピュータ 120
ウエブブラウザ 121
通信仲介プログラム
122
通信モジュール123
購入者携
帯端末
130
通信モジュール 131
ICカード 132
個人識別情報
133

図2

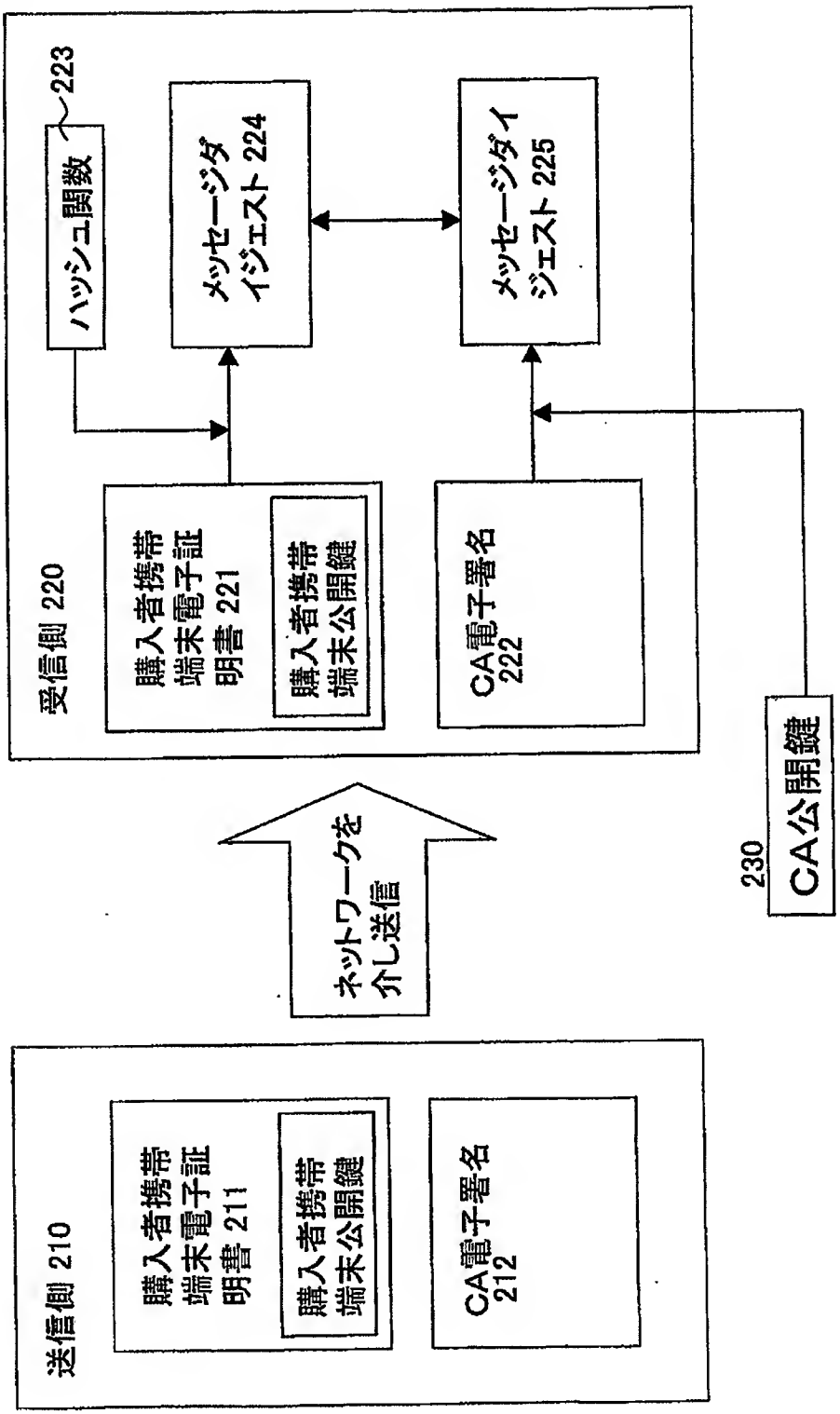

送信側 210
購入者携帯端末電子証明書 211
購入者携帯端末公開鍵
CA電子署名 212
ネットワークを介し送信
受信側 220
購入者携帯端末電子証明書 221
購入者携帯端末公開鍵
CA電子署名 222
ハッシュ関数 223
メッセージダイジェスト 224
メッセージダイジェスト 225
230 CA公開鍵

図3

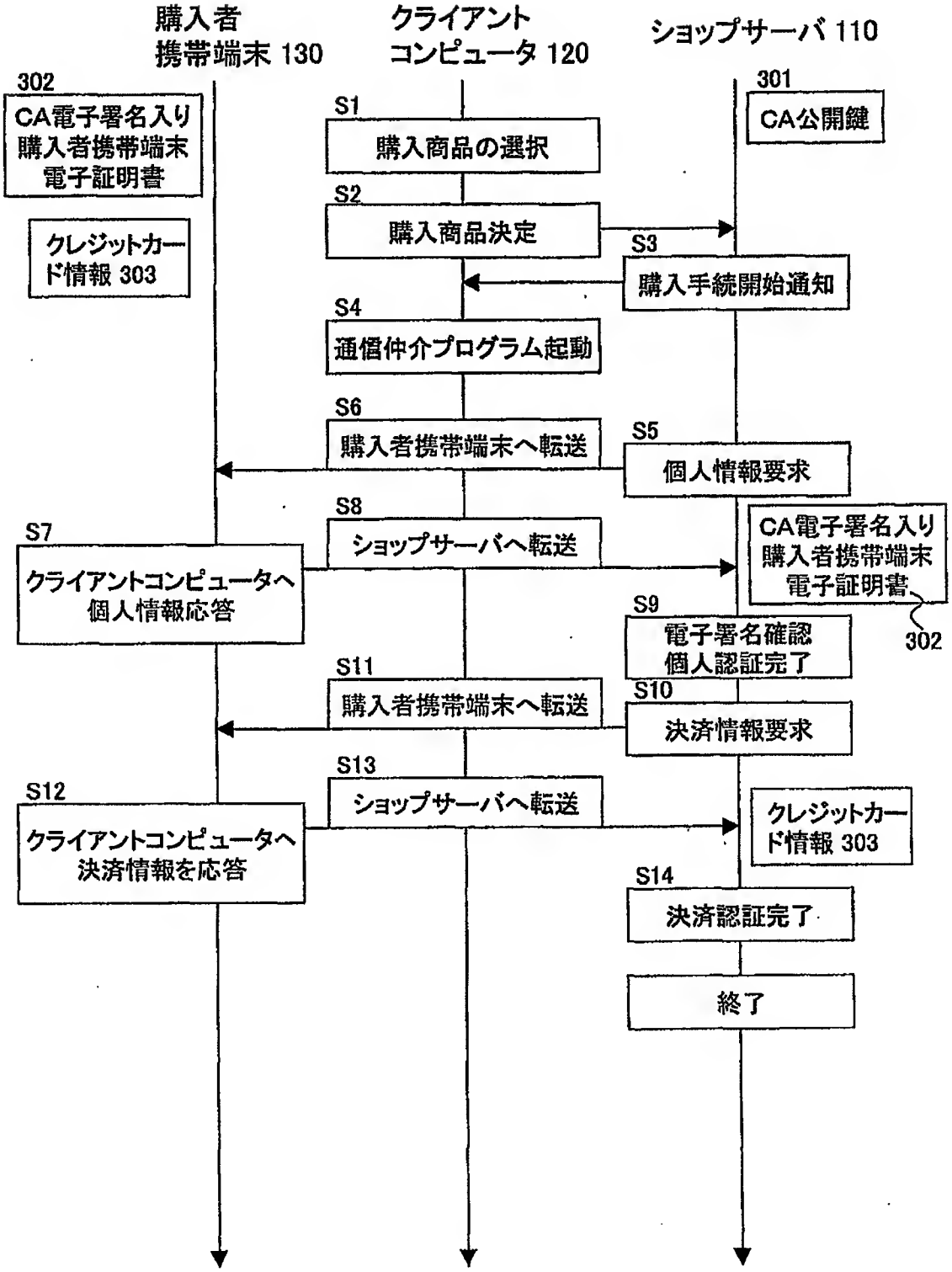

購入者
携帯端末 130
クライアント
コンピュータ 120
ショップサーバ 110
302
CA電子署名入り
購入者携帯端末
電子証明書
クレジットカード情報 303
301
CA公開鍵
S1
購入商品の選択
S2
購入商品決定
S3
購入手続開始通知
S4
通信仲介プログラム起動
S6
購入者携帯端末へ転送
S5
個人情報要求
S8
ショップサーバへ転送
S7
クライアントコンピュータへ
個人情報応答
CA電子署名入り
購入者携帯端末
電子証明書
302
S9
電子署名確認
個人認証完了
S11
購入者携帯端末へ転送
S10
決済情報要求
S13
ショップサーバへ転送
S12
クライアントコンピュータへ
決済情報を応答
クレジットカード情報 303
S14
決済認証完了
終了

図4

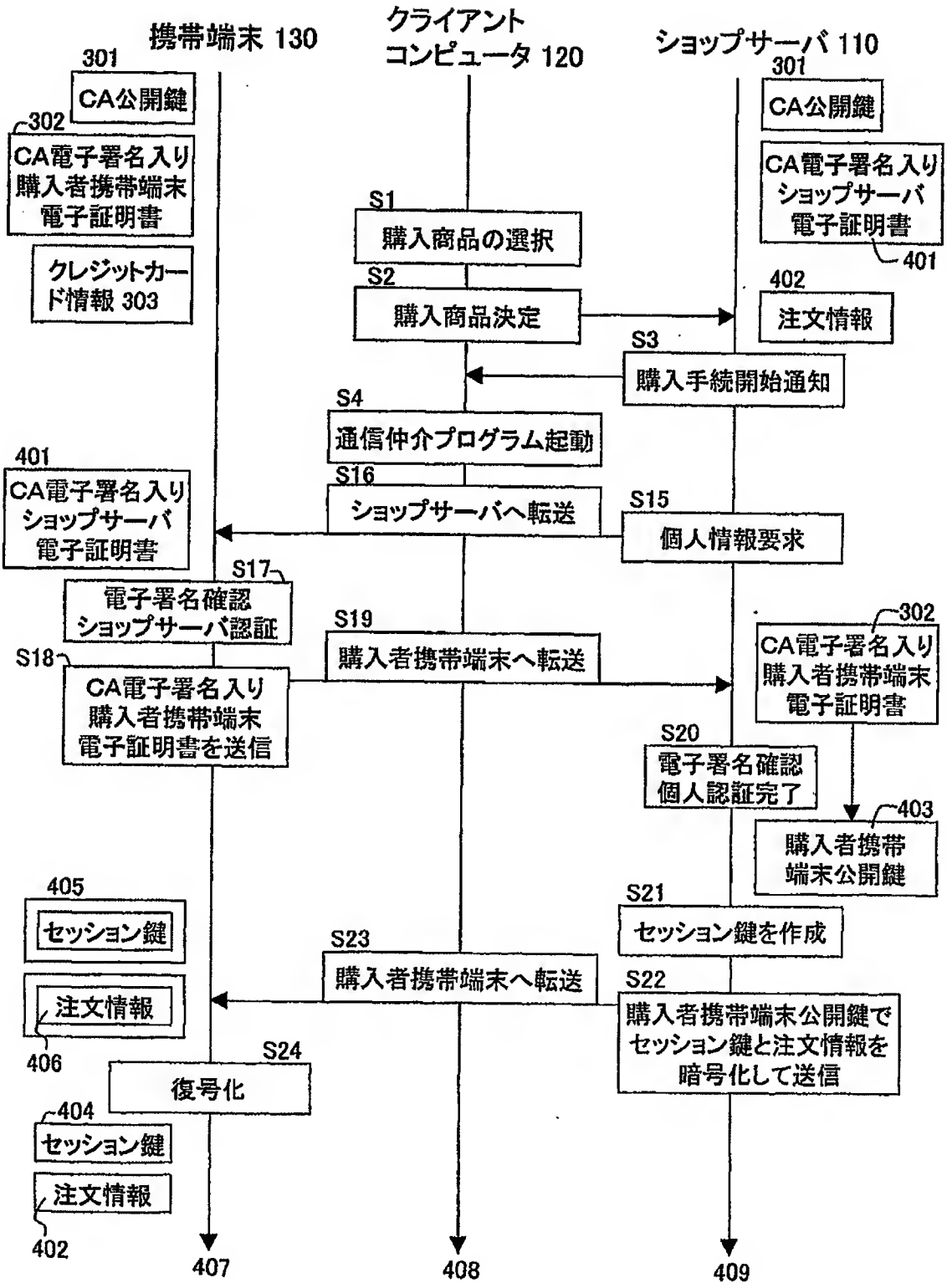

携帯端末 130
クライアント
コンピュータ 120
ショップサーバ 110
301
CA公開鍵
302
CA電子署名入り
購入者携帯端末
電子証明書
クレジットカード情報 303
301
CA公開鍵
CA電子署名入り
ショップサーバ
電子証明書
401
S1
購入商品の選択
S2
購入商品決定
402
注文情報
S3
購入手続開始通知
S4
通信仲介プログラム起動
401
CA電子署名入り
ショップサーバ
電子証明書
S16
ショップサーバへ転送
S15
個人情報要求
S17
電子署名確認
ショップサーバ認証
S19
購入者携帯端末へ転送
302
CA電子署名入り
購入者携帯端末
電子証明書
S18
CA電子署名入り
購入者携帯端末
電子証明書を送信
S20
電子署名確認
個人認証完了
403
購入者携帯
端末公開鍵
405
セッション鍵
S21
セッション鍵を作成
S23
購入者携帯端末へ転送
注文情報
406
S22
購入者携帯端末公開鍵で
セッション鍵と注文情報を
暗号化して送信
S24
復号化
404
セッション鍵
注文情報
402
407
408
409

図5

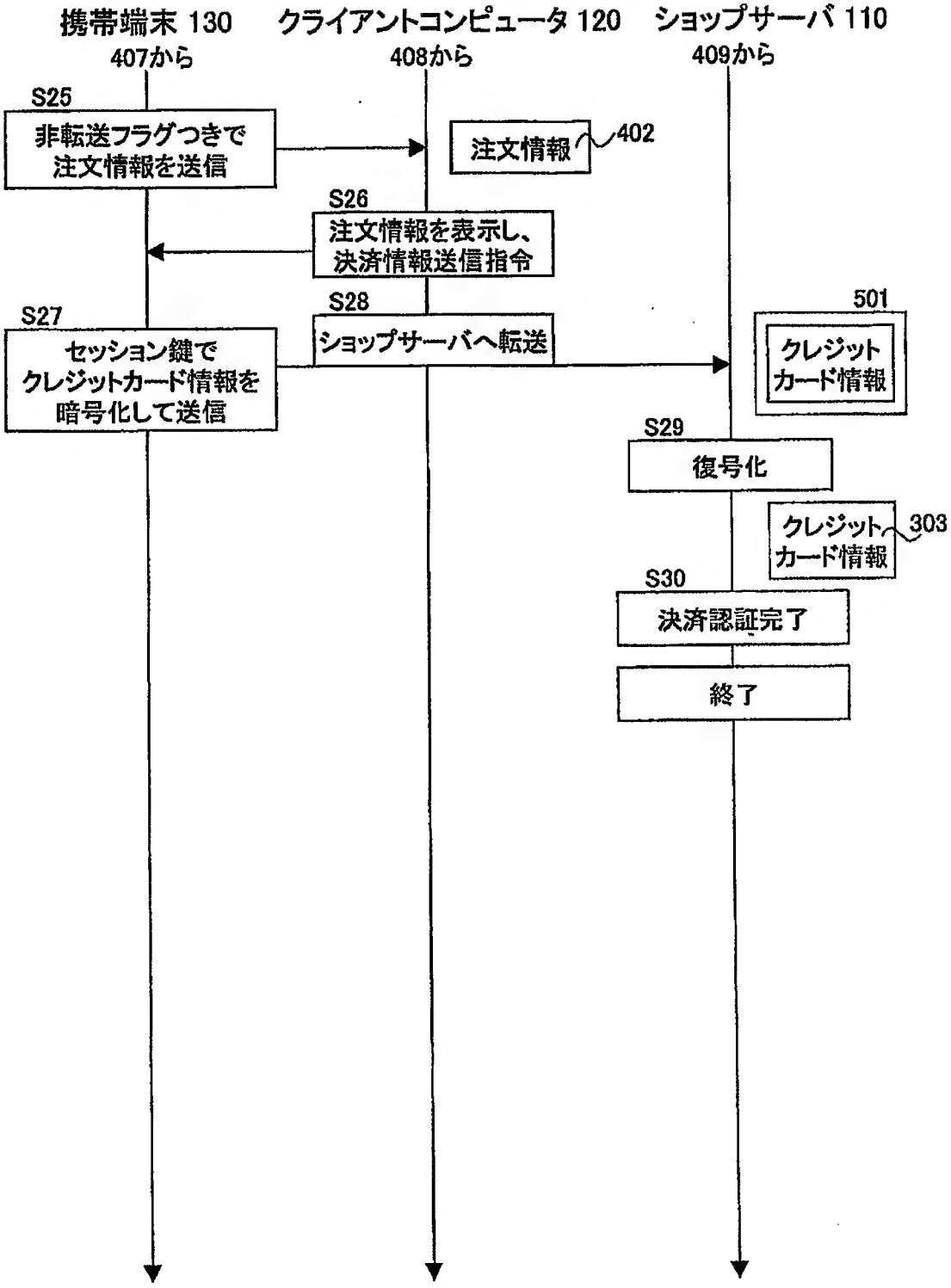

携帯端末 130
クライアントコンピュータ 120
ショップサーバ 110
407から
408から
409から
S25
非転送フラグつきで
注文情報を送信
注文情報
402
S26
注文情報を表示し、
決済情報送信指令
S27
セッション鍵で
クレジットカード情報を
暗号化して送信
S28
ショップサーバへ転送
501
クレジット
カード情報
S29
復号化
クレジット
カード情報
303
S30
決済認証完了
終了

図6

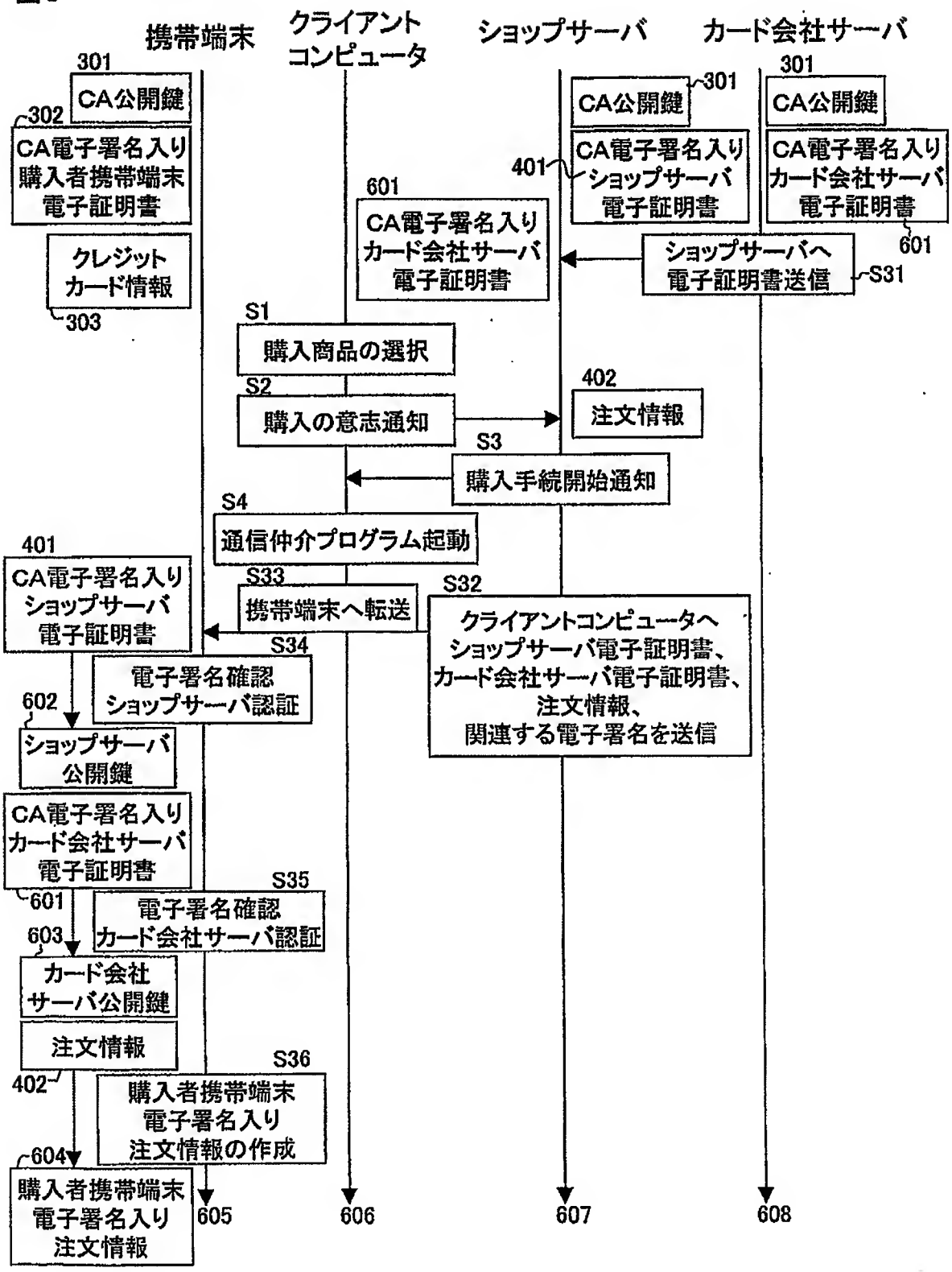

携帯端末
クライアントコンピュータ
ショップサーバ
カード会社サーバ
301
CA公開鍵
302
CA電子署名入り購入者携帯端末電子証明書
クレジットカード情報
303
601
CA電子署名入りカード会社サーバ電子証明書
401
CA電子署名入りショップサーバ電子証明書
ショップサーバへ電子証明書送信
S31
S1
購入商品の選択
S2
購入の意志通知
402
注文情報
S3
購入手続開始通知
S4
通信仲介プログラム起動
S33
携帯端末へ転送
S32
クライアントコンピュータへショップサーバ電子証明書、カード会社サーバ電子証明書、注文情報、関連する電子署名を送信
S34
電子署名確認ショップサーバ認証
602
ショップサーバ公開鍵
S35
電子署名確認カード会社サーバ認証
603
カード会社サーバ公開鍵
注文情報
S36
購入者携帯端末電子署名入り注文情報の作成
604
購入者携帯端末電子署名入り注文情報
605
606
607
608

図7

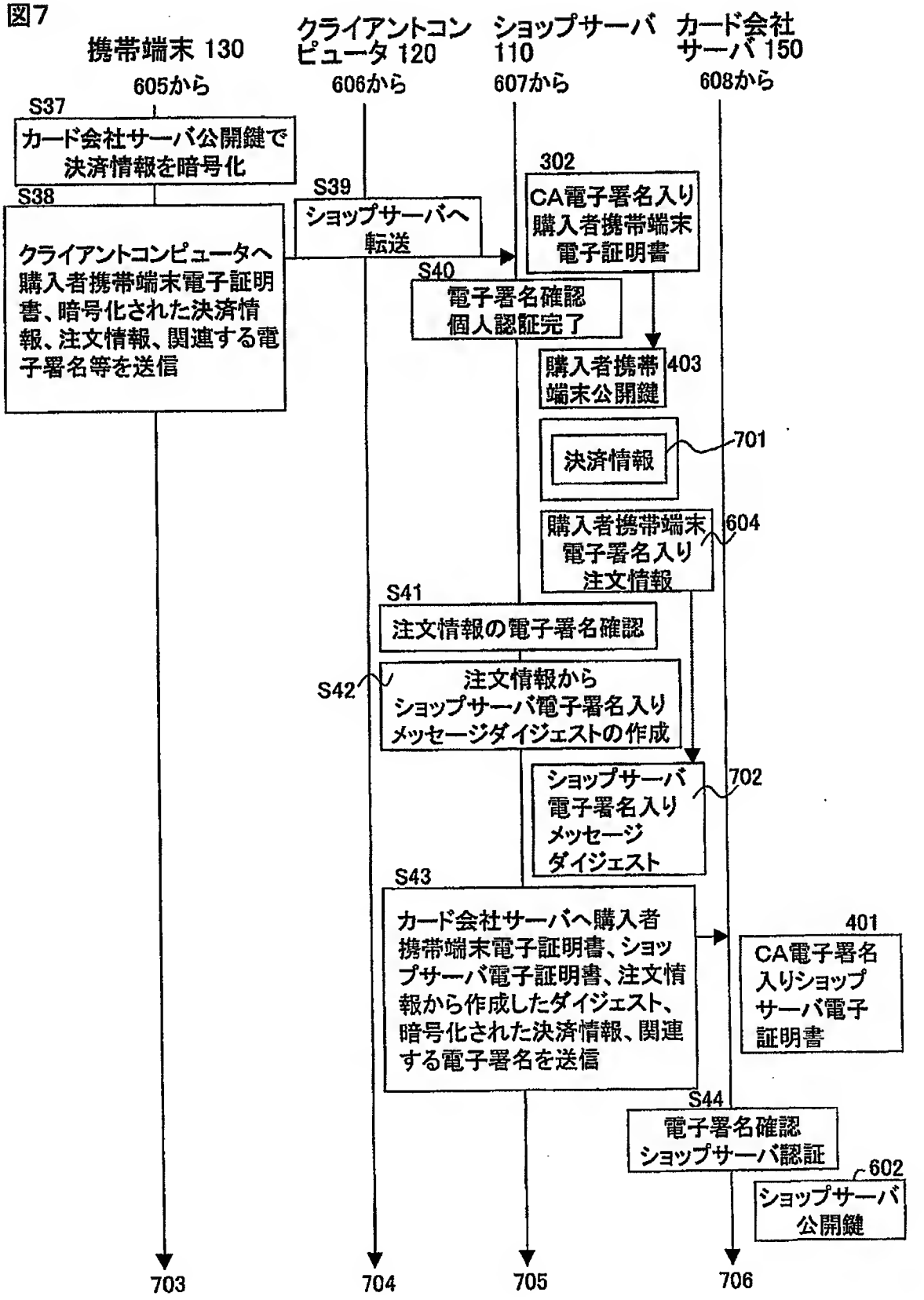

携帯端末 130
クライアントコンピュータ 120
ショップサーバ 110
カード会社サーバ 150
605から
606から
607から
608から
S37
カード会社サーバ公開鍵で決済情報を暗号化
S38
クライアントコンピュータへ購入者携帯端末電子証明書、暗号化された決済情報、注文情報、関連する電子署名等を送信
S39
ショップサーバへ転送
302
CA電子署名入り購入者携帯端末電子証明書
S40
電子署名確認個人認証完了
購入者携帯端末公開鍵
403
決済情報
701
購入者携帯端末電子署名入り注文情報
604
S41
注文情報の電子署名確認
S42
注文情報からショップサーバ電子署名入りメッセージダイジェストの作成
ショップサーバ電子署名入りメッセージダイジェスト
702
S43
カード会社サーバへ購入者携帯端末電子証明書、ショップサーバ電子証明書、注文情報から作成したダイジェスト、暗号化された決済情報、関連する電子署名を送信
401
CA電子署名入りショップサーバ電子証明書
S44
電子署名確認ショップサーバ認証
602
ショップサーバ公開鍵
703
704
705
706

図8

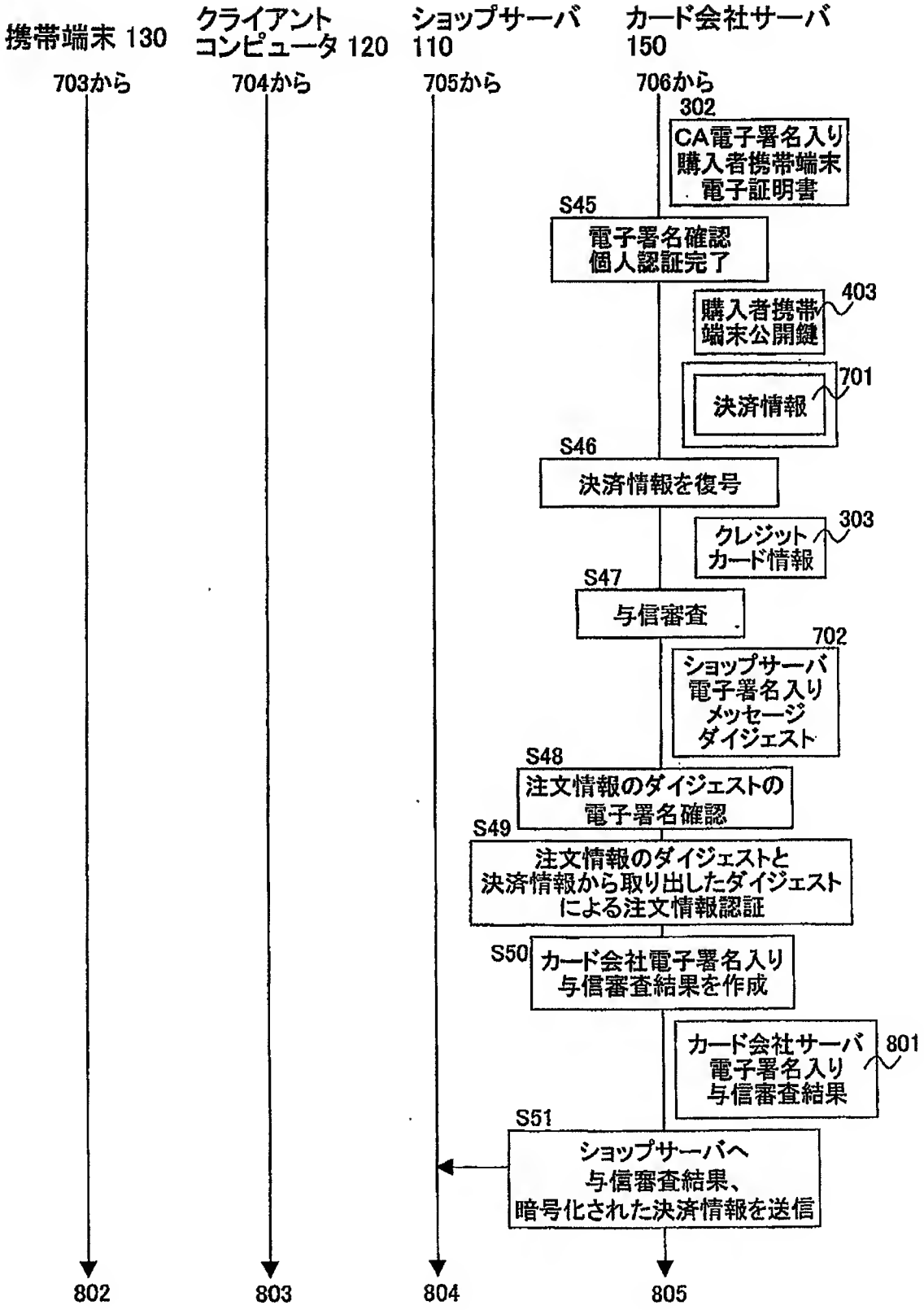
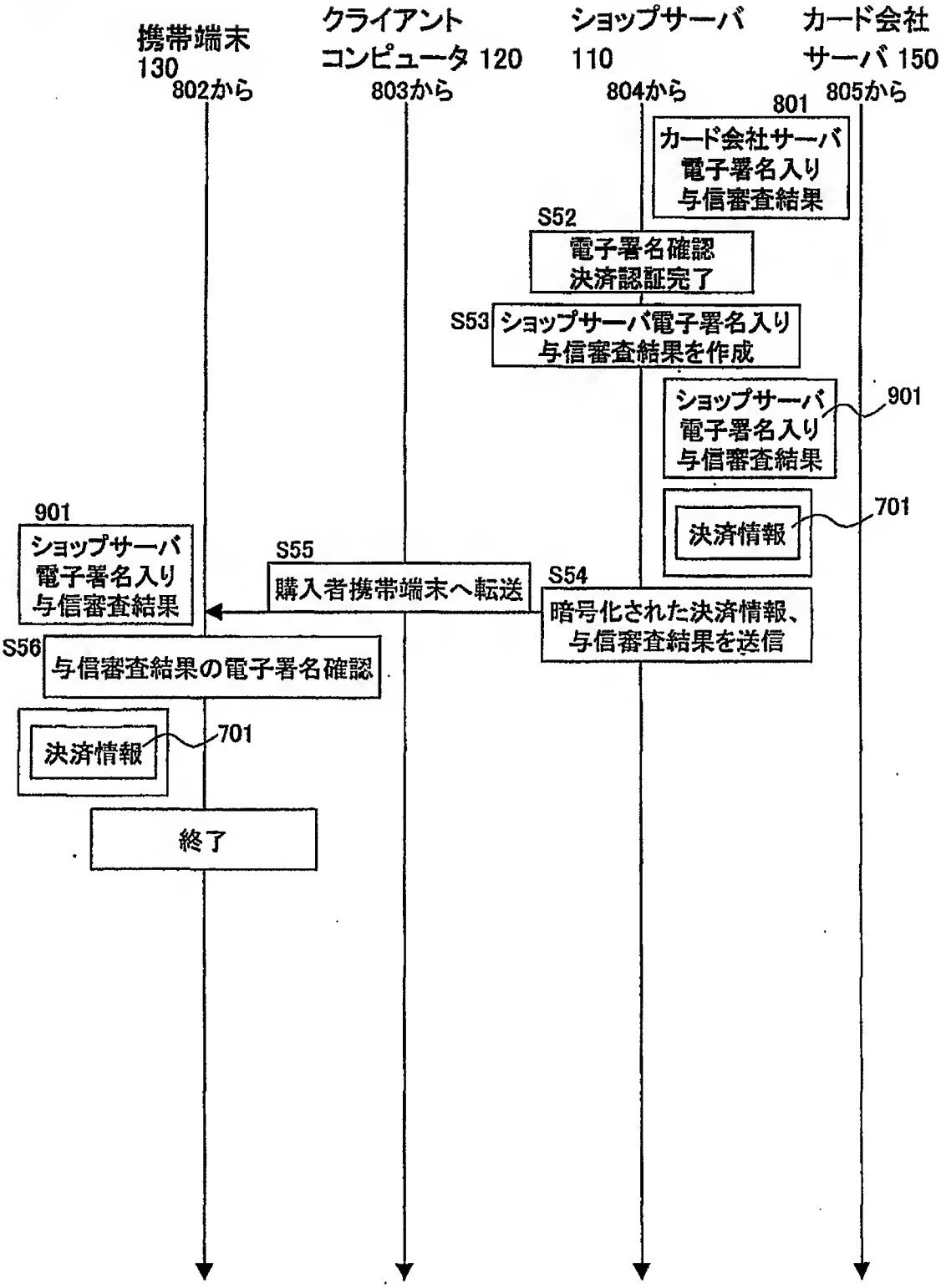

携帯端末 130
クライアント コンピュータ 120
ショップサーバ 110
カード会社サーバ 150
703から
704から
705から
706から
302
CA電子署名入り購入者携帯端末電子証明書
S45
電子署名確認 個人認証完了
403
購入者携帯端末公開鍵
701
決済情報
S46
決済情報を復号
303
クレジットカード情報
S47
与信審査
702
ショップサーバ電子署名入りメッセージダイジェスト
S48
注文情報のダイジェストの電子署名確認
S49
注文情報のダイジェストと決済情報から取り出したダイジェストによる注文情報認証
S50
カード会社電子署名入り与信審査結果を作成
801
カード会社サーバ電子署名入り与信審査結果
S51
ショップサーバへ与信審査結果、暗号化された決済情報を送信
802
803
804
805

図9


携帯端末 130
802から
クライアント コンピュータ 120
803から
ショップサーバ 110
804から
カード会社 サーバ 150
805から
801
カード会社サーバ 電子署名入り 与信審査結果
S52
電子署名確認 決済認証完了
S53
ショップサーバ電子署名入り 与信審査結果を作成
ショップサーバ 電子署名入り 与信審査結果
901
決済情報
701
901
ショップサーバ 電子署名入り 与信審査結果
S55
購入者携帯端末へ転送
S54
暗号化された決済情報、 与信審査結果を送信
S56
与信審査結果の電子署名確認
決済情報
701
終了

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP02/05582

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F17/60; G06K17/00, G06K19/07

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2002
Kokai Jitsuyo Shinan Koho	1971-2002	Jitsuyo Shinan Toroku Koho	1996-2002

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6182900 B1 (Siemens Nixdorf Informationssysteme AG.), 06 February, 2001 (06.02.01), Column 5, lines 34 to 50 & AU 63910/98 A & DE 19710249 A1 & EP 0970447 A2 & JP 2001-515621 A & WO 98/40851 A2	1-9
Y	JP 2000-138672 A (NTT Data Corp.), 16 May, 2000 (16.05.00), Fig. 3 (Family: none)	1-9
Y	EP 1030272 A2 (Matsushita Electric Industrial Co., Ltd.), 23 August, 2000 (23.08.00), Fig. 6 & JP 2000-306003 A	1-9

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 10 September, 2002 (10.09.02)	Date of mailing of the international search report 08 October, 2002 (08.10.02)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP02/05582

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2002-083243 A (Dainippon Printing Co., Ltd.), 22 March, 2002 (22.03.02), Fig. 1 (Family: none)	1-9

国際調査報告

国際出願番号 PCT/JP02/05582

A. 発明の属する分野の分類（国際特許分類（IPC））

Int. Cl.[7] G06F17/60

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl.[7] G06F17/60; G06K17/00, G06K19/07

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922–1996年
日本国公開実用新案公報	1971–2002年
日本国登録実用新案公報	1994–2002年
日本国実用新案登録公報	1996–2002年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	US 6182900 B1 (SIEMENS NIXDORF INFORMATIONSSYSTEME AG) 2001.02.06 *コラム5, 34–50行* & AU 63910/98 A & DE 19710249 A1 & EP 0970447 A2 & JP 2001-515621 A & WO 98/40851 A2	1–9

☒ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 10.09.02	国際調査報告の発送日 03.10.02
国際調査機関の名称及びあて先 日本国特許庁（ISA/JP） 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 阿波 進 5L 9168 電話番号 03-3581-1101 内線 3561

様式PCT/ISA/210（第2ページ）（1998年7月）

国際調査報告

国際出願番号 PCT／JP02／05582

C（続き）. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 2000-138672 A (株式会社エヌ・ティ・ティ・データ) 2000.05.16 *図3* (ファミリーなし)	1-9
Y	EP 1030272 A2 (MATSUSHITA ELECTRIC INDUSTRY CO., LTD.) 2000.08.23 *図6* & JP 2000-306003 A	1-9
Y	JP 2002-083243 A (大日本印刷株式会社) 2002.03.22 *図1* (ファミリーなし)	1-9